První certifikační autorita, a.s.

Politika

vydávání prostředků pro bezpečné vytváření elektronických podpisů

Politika vydávání prostředků pro bezpečné vytváření elektronických podpisů je veřejným dokumentem, který je vlastnictvím společnosti První certifikační autorita, a.s., a byl vypracován jako nedílná součást komplexní bezpečnostní dokumentace. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu majitele autorských práv.

Verze 1.4

Copyright © První certifikační autorita, a.s.

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	březen 2011	Ředitel společnosti První certifikační autorita, a.s.	První vydání, čipová karta Starcos 3.0.
1.1	17.08.2015	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace dokumentu s ohledem na čipovou kartu Starcos 3.2.
1.2	22.04.2016	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace dokumentu s ohledem na čipovou kartu Starcos 3.5.
1.3	20.03.2017	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace s ohledem na eIDAS.
1.4	21.04.2021	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace dokumentu s ohledem na novou čipovou kartu Starcos 3.7, kontrola uvedení SSCD na důvěryhodném seznamu, formální změny.

1 Úvod

Podle článku 51 „Přechodná ustanovení" bodu 1 **Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES** (dále eIDAS) platí:

- Prostředky pro bezpečné vytváření podpisu, jejichž shoda byla stanovena podle čl. 3 odst. 4 směrnice 1999/93/ES, se považují za kvalifikované prostředky pro vytváření elektronických podpisů podle tohoto nařízení.

S ohledem na výše uvedené je v následujících kapitolách pod pojmem „Secure Signature Creation Device" (SSCD) míněn i pojem „Qualified Signature Creation Device" (QSCD).

1.1 Přehled

Dokument **Politika vydávání prostředků pro bezpečné vytváření elektronických podpisů** (dále též Politika), vypracovaný společností První certifikační autorita, a. s., (dále též I.CA), vztahující se ke službě vydávání SSCD (dále též Služba), je rozdělen do deseti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 definuje požadavky na prostředky pro bezpečné vytváření elektronických podpisů, popisuje způsob zveřejňování informací.
- Kapitola 2 popisuje činnosti vztahující se k SSCD při jejich převzetí, personalizací a předání koncovým uživatelům a dále činnosti koncového uživatele.
- Kapitoly 3 až 6 popisují opatření v oblastech fyzické, procesní, personální a technické bezpečnosti.
- Kapitola 7 je zaměřena na problematiku auditních záznamů.
- Kapitola 8 definuje množinu zaznamenávaných událostí a jejich uchovávání.
- Kapitola 9 zahrnuje problematiku obchodní a právní.
- Kapitola 10 obsahuje přílohy.

1.2 Správa dokumentu

Tuto Politiku spravuje společnost První certifikační autorita, a.s.

1.3 Použité pojmy a zkratky

tab. 2 - Pojmy a zkratky

Pojem	Vysvětlení
bit	z anglického *binary digit* – číslice dvojkové soustavy je základní a současně nejmenší jednotkou informace používanou především v číslicové a výpočetní technice
CA	certifikační autorita
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické

	transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
elektronický podpis	elektronický podpis, nebo zaručený elektronický podpis, nebo kvalifikovaný elektronický podpis, nebo uznávaný elektronický podpis dle právní úpravy pro služby vytvářející důvěru
kořenový certifikát	self-signed certifikát certifikační autority na vrcholu hierarchické struktury certifikačních autorit
kvalifikovaná služba vytvářející důvěru	služba vytvářející důvěru, která splňuje požadavky stanovené v eIDAS
kvalifikovaný certifikát pro elektronický podpis	certifikát definovaný právní úpravou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II eIDAS
párová data	jedinečná data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu
PIN	Personal Identification Number, autentizační kód/číslo uživatele
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
právní úprava pro služby vytvářející důvěru	právní předpisy České republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
PUK	Personal Unlocking Key, autentizační kód/číslo pro odblokování PIN uživatele (zablokovaného po třikrát opakovaně chybně zadaném PIN)
RA	registrační autorita
self-signed certifikát	certifikát veřejného klíče podepsaný soukromým klíčem tvořícím s tímto veřejným klíčem párová data
soukromý klíč	jedinečná data pro vytváření elektronického podpisu
SSCD	Secure Signature Creation Device, prostředek pro bezpečné vytváření elektronického podpisu
QSCD	Qualified Signature Creation Device, kvalifikovaný prostředek pro bezpečné vytváření elektronického podpisu
veřejný klíč	jedinečná data pro ověřování elektronického podpisu
zákon o ochraně utajovaných informací	zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
ZOOÚ	právní úprava týkající se ochrany osobních údajů

1.4 Zveřejňování informací

Základní adresy, na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s., případně odkazy pro zjištění dalších informací, jsou:

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- internetová adresa http://www.ica.cz,
- sídla registračních autorit.

I.CA zveřejňuje výše uvedené kontaktní adresy na své internetové adrese a pracovištích RA. Pracovníci RA, včetně smluvních partnerů, jsou rovněž povinni tyto informace na vyžádání sdělit veřejnosti.

2 Bezpečný prostředek pro tvorbu elektronického podpisu

Prostředky pro bezpečné vytváření elektronických podpisů, které I.CA., vydává koncovým uživatelům, jsou plastové karty obsahující čip s operačním systémem Starcos 3.0/3.2/3.5/3.7 výrobce Giesecke & Devrient GmbH, splňující požadavky eIDAS kladené na tyto prostředky. Zkratka SSCD ve zbytku dokumentu označuje tyto konkrétní prostředky.

Činnosti související s vydáváním SSCD jsou prováděny s využitím vyhrazeného informačního systému s autentizací na bázi PKI (dále Systém).

2.1 Získání SSCD od dodavatele

I.CA zašle dodavateli poptávku na dodání SSCD obsahující:

- specifikaci požadovaného počtu,
- specifikaci materiálu čipové karty,
- specifikaci potisku,
- podmínku, že SSCD musí být uvedeno na důvěryhodném seznamu některé z členských zemí EU s dobou platnosti (SSCD designation expiry) minimálně dvou let.
- případně žádost o rozšíření pro bezkontaktní komunikační rozhraní.

Po vzájemném odsouhlasení konečné podoby karty (design, umístění čipu) následuje výroba požadovaného množství. Hotové čipové karty jsou potom v sídle dodavatele pracovníkem I.CA osobně a protokolárně převzaty, převezeny do skladu I.CA a zaevidovány v Systému. Podrobný popis postupů, prováděných při získání SSCD od dodavatele, je uveden v interní dokumentaci.

2.2 Ořez čipu SSCD

V případě, že je požadován výřez pro formát umožňující umístění čipové části s kontakty do USB tokenu, nebo do malých USB čteček (tzv. punching), je prostřednictvím přepravní společností odesláno sjednané množství čipových karet zpracovateli, odeslání je evidováno v Systému Zpracovatel provede punching a odeslání čipů zpět, přijetí je evidováno v Systému. Podrobný popis postupů, vztahujících se k prováděných výřezu z formátu čipové karty, je uveden v interní dokumentaci I.CA.

2.3 Personalizace

Postupy, prováděné v procesu personalizace, jsou podrobně popsány v interní dokumentaci.

2.3.1 Zadání požadavku

Pověřený pracovník I.CA v Systému definuje zákaznický profil obsahující parametry, nutné pro personalizaci dávky SSCD. Na základě zvoleného zákaznického profilu je každému SSCD přiřazeno jedinečné šestnáctimístné identifikační číslo, obsahující ve druhém čtyřčíslí kód tohoto profilu. Výsledkem je vytvoření personalizačního souboru, obsahujícího veškeré potřebné informace.

2.3.2 Přeprava SSCD na provozní pracoviště

Samotný proces personalizace SSCD je prováděn na provozním pracovišti I.CA, jehož zabezpečení je popsáno v kapitole 3.1. Pověřený pracovník I.CA proto překontroluje, zda je požadované množství SSCD na provozním pracovišti k dispozici. V případě, že provozní pracoviště požadovaným množstvím SSCD nedisponuje, zajistí jejich přepravu (prostřednictvím přepravní společnosti nebo zaměstnancem I.CA) ze skladu I.CA. Přesun je evidován v Systému.

2.3.3 Realizace

Při personalizaci nejsou v SSCD generovány žádné soukromé klíče koncového uživatele, tyto si generuje koncový uživatel až ve fázi používání SSCD – viz kap. 2.5.2. Pověřený pracovník provozního pracoviště získá ze Systému příslušný personalizační soubor (viz kap. 2.3.1), který uloží do personalizačního zařízení. Při personalizaci jsou do čipu, popř. na plastové tělo každého SSCD (potisk), uloženy veškeré informace, obsažené v personalizačním souboru.

Standardně jsou SSCD personalizována bez aktivačních dat, tj. PIN a PUK. K zadání PIN a PUK je v tomto případě vlastník SSCD vyzván při prvním použití SSCD. V případě obráceném, kdy PIN a PUK generovány jsou, jsou tyto tištěny do bezpečnostních PIN obálek, nebo na papírový nosič, kde jsou následně přelepeny certifikovanou bezpečnostní páskou.

Personalizované karty, případně včetně bezpečnostních obálek nebo papírových nosičů s údaji přelepenými certifikovanou bezpečnostní páskou, jsou, prostřednictvím přepravní společnosti nebo zaměstnance I.CA, přepraveny zpět do skladu I.CA. Přesun je evidován v Systému.

2.4 Předání koncovému uživateli

Požadovaná množství SSCD distribuují pracovníci I.CA na základě předávacího protokolu pracovištím veřejných registračních autorit (evidováno v Systému). Zde jsou SSCD umístěna v konsignačních skladech.

Koncovým uživatelům jsou SSCD předávána spolu s instrukcemi pro instalaci, uvedenými v dokumentu *Pokyny_pro_instalaci.pdf*. Vlastní předání je možné těmito způsoby:

- při objednání prostřednictvím e-shopu I.CA je zákazníkovi poštou zasláno SSCD, vždy se v tomto případě jedná o SSCD personalizované bez aktivačních dat – viz kap. 2.3.3, včetně protokolu o předání,
- při předání na registrační autoritě si koncový uživatel může zvolit, zda se má jednat SSCD personalizované s aktivačními daty, v tomto případě obdrží také papírový nosič s údaji přelepenými certifikovanou bezpečnostní páskou, nebo bez nich, a vždy obdrží také protokol o předání,
- další možností je získání SSCD a bezpečnostní PIN obálky obsahující údaje PIN/PUK na registrační autoritě.

2.5 Používání SSCD koncovým uživatelem

2.5.1 Instalace a inicializace SSCD

Po převzetí SSCD a před zahájením jeho rutinního používání musí koncový uživatel provést následující úkony:

- Instalaci příslušného ovladače čtečky čipové karty. Pokud není po připojení USB čtečky čipové karty automaticky nainstalován odpovídající ovladač, je nutné provést instalaci manuální. Příslušný ovladač lze získat na webové stránce http://ica.cz/Ovladace-HW.
- Stažení aktuální verze aplikace I.CA SecureStore z webové stránky http://ica.cz/Aplikace-stazeni.
- Instalaci aplikace I.CA SecureStore. Postup je uveden v aktuálním instalační příručce, dostupné na webové adrese http://ica.cz/Aplikace-stazeni.
- Pokud byla karta personalizována bez aktivačních dat, inicializovat aktivační data čipové karty, tzn. zadat PIN/PUK (délku minimálně čtyři, maximálně osm numerických znaků).

2.5.2 Používání SSCD

Po provedení úkonů, uvedených v kapitole 2.5.1, je SSCD připraveno pro rutinní využívání, včetně jeho správy. Postupy pro správu, generování párových dat (veřejný a soukromý klíč), vytvoření žádosti o certifikát a instalaci certifikátu jsou popsány v aktuální uživatelské příručce dostupné na webové adrese http://ica.cz/Aplikace-stazeni.

2.6 Kontrola uvedení na seznamu SSCD/QSCD prostředků

Pověřený pracovník I.CA provádí jednou měsíčně kontrolu unijního seznamu SSCD/QSCD prostředků (EU Trust Services Dashboard (europa.eu)), zda na něm používaná SSCD zařízení (viz úvod kapitoly 2) uvedena jsou, Provedení kontroly zaznamená v billingovém systému I.CA do k tomuto účelu zřízené tabulky. Pokud došlo ke změně, informuje prokazatelně garanta systému vydávání certifikátů a bezpečnostního manažera I.CA.

2.7 Vyřazení ze seznamu SSCD/QSCD prostředků v průběhu platnosti certifikátu

Pokud v průběhu platnosti certifikátu dojde ke změně a zařízení je vyjmuto ze seznamu SSCD/QSCD, je postupováno stejným způsobem, jako při zjištění duplicity soukromého klíče (certifikát je zneplatněn, zákazníkovi je nabídnuto zakoupení jiného zařízení QSCD a bezplatně je mu vydán nový certifikát).

3 Fyzická bezpečnost

3.1 I.CA – provozní pracoviště

Níže jsou uvedena zásadní pravidla pro zabezpečení provozního pracoviště. Konkrétní fyzická, procesní a personálními opatření, implementovaná pro zabezpečení provozního pracoviště, jsou popsána v interní dokumentaci.

3.1.1 Umístění a konstrukce

Procesy, spojené s personalizací čipových karet (viz kap. 2.3.3), jsou prováděny v objektu provozního pracoviště, který je umístěn v geograficky odlišné lokalitě, než jsou ředitelství společnosti, obchodní a vývojová pracoviště, pracoviště registračních autorit a obchodních míst. Zařízení určená k personalizaci SSCD jsou umístěna ve vyhrazeném prostoru tohoto provozního pracoviště, který je zabezpečen obdobně, jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona o ochraně utajovaných informací.

3.1.2 Fyzický přístup

Fyzický přístup do prostor, kde je prováděna personalizace SSCD, je chráněn mechanickými a elektronickými prostředky. Ochrana objektu je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a speciálním systémem pro snímání, zobrazování a zaznamenávání pohybu osob a dopravních prostředků. Podrobnosti jsou popsány v interní dokumentaci.

3.1.3 Elektřina

Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

3.1.4 Vlivy vody

Všechny systémy Služby jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště je vybaveno čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

3.1.5 Protipožární opatření a ochrana

V objektu provozního pracoviště je instalována elektronická požární signalizace (EPS) připojená na pult centrální ochrany. Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení Služby, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

3.1.6 Ukládání médií

Čipové karty a případně obálky s PIN/PUK jsou umístěny v zabezpečeném prostoru, kde jsou umístěna zařízení určená k personalizaci těchto karet – viz kap. 3.1.1.

3.2 Sklad I.CA

Pokud jsou SSCD uložena ve skladu I.CA, jedná se o fyzicky zabezpečené prostory s přístupem povoleným pouze pověřeným zaměstnancům I.CA. Fyzická, procesní

a personální opatření, implementovaná pro zabezpečení těchto prostor, jsou popsána v interní dokumentaci.

4 Procesní bezpečnost

4.1 Důvěryhodné role

Činnosti týkající se personalizace SSCD provádějí pracovníci I.CA zařazení v systémech pro poskytování certifikačních služeb do důvěryhodných rolí. Tyto role jsou, spolu s odpovídajícími činnostmi a odpovědnostmi, popsány v interní dokumentaci.

4.2 Identifikace a autentizace

Pracovníkům podílejícím se na poskytování Služby a na činnosti Sytému jsou přiděleny prostředky pro řádnou identifikaci a autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné.

5 Personální bezpečnost

5.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Pracovníci I.CA v důvěryhodných rolích jsou vybíráni a přijímáni na základě těchto kritérií:

- naprostá občanská bezúhonnost – prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z rejstříku trestů nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně tři roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně pět let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně jeden rok v oblasti poskytování certifikačních služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní pracovníci I.CA podílející se na zajištění Služby jsou přijímáni na základě následujících kritérií:

- vysokoškolské vzdělání v rámci akreditovaného bakalářského, resp. magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

5.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

- sami tito zaměstnanci,
- osoby, které tyto zaměstnance znají,
- veřejné zdroje informací.

Zaměstnanci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, které jsou aktualizovány při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru.

5.3 Postihy za neoprávněné činnosti zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem uvedeným v interních dokumentech společnosti a řídícím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.4 Požadavky na nezávislé zhotovitele (dodavatele)

I.CA může nebo musí některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. V případě porušení povinností stanovených těmito smlouvami jsou uplatňovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

6 Technická bezpečnost

6.1 SSCD

tab. 3 – Parametry a hodnocení

	Starcos 3.0	**Starcos 3.2**	**Starcos 3.5**	**Starcos 3.7**
Chip	NXP MX P5CT072 NXP MX P5CC072	Infineon SLE66CX680PE	Infineon M7820	Infineon SLC52GDA448
EEPROM	72 kB	68 kB	do 128 kB	448 kB
Maximální délka klíče	2048 bitů/RSA	2048 bitů/RSA 256 bitů/ECC	4096 bitů/RSA 521 bitů/ECC	4096 bitů/RSA 384 bitů/ECDSA
Certifikace čipové karty	Common Criteria EAL 5+	Common Criteria EAL 5+	Common Criteria EAL 5+, ALC_DVS.2, AVA_VAN.5	Common Criteria EAL 6+, ALC_FLR.1
Certifikace OS	Bezpečnostní funkce Common Criteria EAL 4+ Secure Signature Creation Devices (SSCDs)	Bezpečnostní funkce Common Criteria EAL 4+ Secure Signature Creation Devices (SSCDs)	Bezpečnostní funkce Common Criteria EAL4+, AVA_VAN.5 Secure Signature Creation Devices (SSCDs)	Bezpečnostní funkce Common Criteria EAL4+, AVA_VAN.5 Secure Signature Creation Devices (SSCDs)

6.2 Počítačová bezpečnost

Úroveň bezpečnosti použitých komponent je definována technickými standardy.

6.3 Síťová bezpečnost

Vyhrazený Systém ani personalizační zařízení nejsou přímo dostupné z veřejné sítě Internet, jsou mimo jiné chráněny firewallem.

7 Auditní záznamy

7.1 Typy zaznamenávaných událostí

V Systému jsou evidovány události související s jeho činností, zejména:

- spuštění a ukončení systému,
- spuštění a ukončení funkcí auditu,
- změny parametrů auditu,
- akce, prováděné při chybách úložiště auditních záznamů,
- všechny pokusy přístupu k systému.

Záznamy v auditním souboru obsahují následující parametry:

- datum a čas události,
- typ události,
- identitu entity, která je za akci odpovědná.

Auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze na definované uživatele.

7.2 Doba uchování auditních záznamů

Nestanoví-li relevantní právní úprava jinak, jsou auditní záznamy uchovávány po dobu nejméně 10 let od jejich vzniku.

7.3 Ochrana auditních záznamů

Auditní záznamy jsou uloženy způsobem, zajišťujícím ochranu před jejich změnami, odcizením a zničením (ať již úmyslným, nebo neúmyslným).

Auditní záznamy jsou ukládány ve dvou kopiích, každá kopie je umístěna v jiné místnosti provozního pracoviště. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno v trezoru mimo provozní prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci.

7.4 Postupy pro zálohování auditních záznamů

Zálohování auditních záznamů probíhá obdobným způsobem, jako zálohování ostatních elektronických informací.

7.5 Systém shromažďování auditních záznamů

Systém shromažďování auditních záznamů je z pohledu informačních systémů interní.

8 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle požadavků právní úpravy pro služby vytvářející důvěru.

8.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává níže uvedené typy informací a dokumentace (v elektronické nebo listinné podobě), které souvisejí se službou vydávání SSCD, zejména:

- aplikační programové vybavení, provozní a bezpečnostní dokumentaci,
- záznamy o manipulaci s SSCD (např. převzetí, předání, uložení atd.).

8.2 Doba uchování uchovávaných informací a dokumentace

Informace dle kap. 8.1 a další dokumentace jsou uchovávány v souladu s kap. 7.2.

Postupy při uchovávání informací a dokumentace jsou upraveny interní dokumentací.

8.3 Ochrana úložiště uchovávaných informací a dokumentace

Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti a zákona o ochraně utajovaných informací.

Postupy při ochraně úložiště uchovávaných informací a dokumentace jsou upraveny interní dokumentací.

8.4 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V případě, že jsou využívána časová razítka, jedná se o časová razítka, vydávaná I.CA.

8.5 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací I.CA.

8.6 Systém shromažďování uchovávaných informací a dokumentace

Informace a dokumentace jsou ukládány na místo určené ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směrnicemi. Shromažďování uchovávaných informací je evidováno.

8.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Uchovávané informace a dokumentace jsou umístěny v k tomu určených lokalitách a jsou přístupné:

- zaměstnancům I.CA, pokud je to k jejich činnosti vyžadováno,
- oprávněným dohledovým a kontrolním subjektům a orgánům činných v trestním řízení a soudům, pokud je to právními normami předpisy vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání SSCD

Poplatky za vydání SSCD jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA.

9.1.2 Jiná ustanovení týkající se poplatků (vč. refundací)

I.CA je oprávněna stanovit pro individuálně uzavřené smlouvy odlišnou výši poplatku za vydání SSCD.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

I.CA prohlašuje, že má uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční škody.

I.CA, sjednala pro všechny zaměstnance pojištění odpovědnosti za škody způsobené zaměstnavateli v rozsahu, určeném představenstvem společnosti.

9.2.2 Další aktiva a záruky

I.CA prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné finanční zajištění s ohledem na riziko vzniku odpovědnosti za škodu při poskytování Služby.

Podrobné informace o aktivech I.CA je možno získat z Výroční zprávy společnosti První certifikační autorita, a.s., zveřejněné v obchodním rejstříku.

9.3 Důvěrnost obchodních informací

9.3.1 Výčet citlivých informací

Důvěrnými informacemi I.CA jsou veškeré informace, které nejsou zveřejňovány způsobem uvedeným v kap. 1.4, zejména:

- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec důvěrných informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kap. 1.4.

9.3.3 Odpovědnost za ochranu důvěrných informací

Žádný pracovník, který přijde do styku s ~~citlivými a~~ důvěrnými informacemi, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů je v I.CA řešena v souladu s požadavky příslušných právních předpisů, tedy zejména ZOOÚ a GDPR.

9.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje podléhající ochraně ve smyslu příslušných právních předpisů.

Zaměstnanci I.CA, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

9.4.3 Údaje, které nejsou považovány za důvěrné

Za citlivé nejsou považovány údaje, které nespadají do působnosti ZOOÚ.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

9.4.5 Oznámení o používání osobních údajů a souhlas s používáním osobních údajů

Problematika oznamování o používání osobních údajů a souhlasu s používáním osobních údajů je v I.CA řešena v souladu s požadavky příslušných právních předpisů.

9.4.6 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní, účely je v I.CA řešeno v souladu s požadavky příslušných zákonných norem veškeré osobní údaje podléhající ochraně ve smyslu příslušných právních předpisů.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně dle požadavků příslušných právních předpisů.

9.5 Práva duševního vlastnictví

Tato Politika, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující vydávání prostředků pro bezpečné vytváření elektronických podpisů, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

9.6 Změny

9.6.1 Postup při změnách

Postup je realizován řízeným procesem popsaným v interním dokumentu.

9.6.2 Postup při oznamování změn

Vydání nové verze tohoto dokumentu je vždy oznámeno formou zveřejňování informací (viz kap. 1.4).

9.7 Rozhodné právo

Obchodní činnost společnosti První certifikační autorita, a.s., se řídí právním řádem České republiky.

9.8 Shoda s právními předpisy

Vydávání SSCD je ve shodě s právními požadavky ČR a EU a dále s relevantními mezinárodními standardy.

9.9 Vyšší moc

I.CA neodpovídá za porušení svých povinností vyplývající ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu nebo vyhlášení stavu ohrožení státu nebo válečného stavu.

10 Přílohy

1. Pokyny_pro_instalaci.pdf